

Abstract

In a digital satellite television system in which a television receives its signal via receiver/decoder, such as a set top box, interactive applications can be downloaded and run on the receiver/decoder. The application code is arranged as modules, and the downloading of modules is preceded by searching a directory module within a specified local address. The modules are signed and the directory module is signed and encrypted so that a single encryption applies to all of the modules making up the application. Multiple public encryption keys are stored in ROM in the receiver/decoder, so that applications can be created by different sources, without the sources needing to know each other's private encryption keys. A facility is provided to enable an encryption key to be temporarily stored in RAM in the receiver/decoder, so that a manufacturer of the receiver/decoder can check its functionality. A signature of the directory may be hidden at a variable position in a block of dummy data in the directory module. An application to be downloaded may be checked against an application validation bitmap stored in the receiver/decoder.

65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100